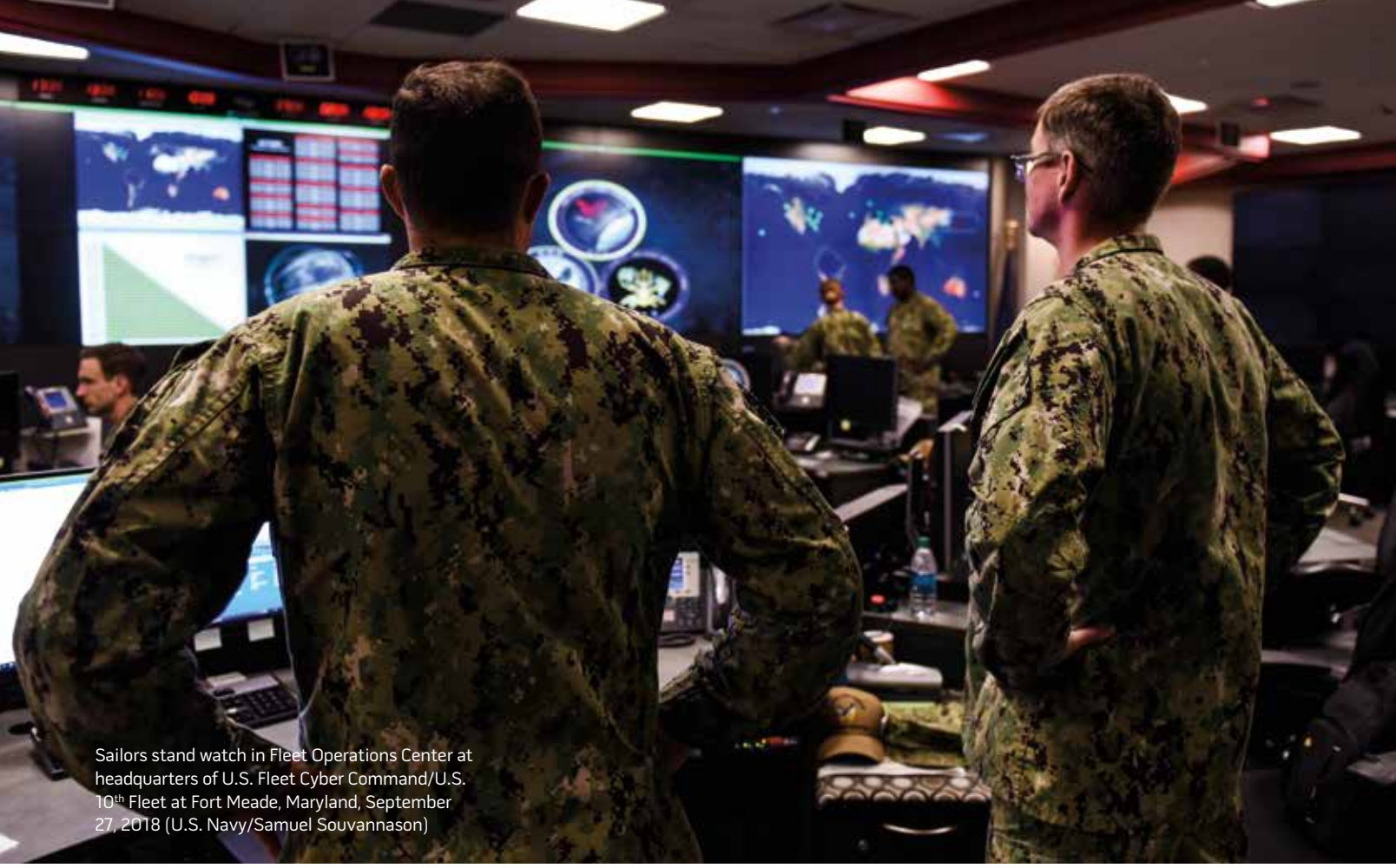

Sailors stand watch in Fleet Operations Center at headquarters of U.S. Fleet Cyber Command/U.S. 10th Fleet at Fort Meade, Maryland, September 27, 2018 (U.S. Navy/Samuel Souvannason)

A Cyber Force for Persistent Operations

By Paul M. Nakasone

Harvard's Samuel Huntington, then just 27, asked the U.S. Navy in 1954, "What function do you perform which obligates society to assume responsibility for your maintenance?" His seminal article in the U.S. Naval Institute's *Proceedings* argued that the basis of a military Service—or any military element—is its purpose or role in implementing national policy. Huntington called this a Service's "strategic concept," which justifies public support by explaining how, when, and where that military arm expects to protect the Nation.[1]

Huntington's question resonated because the Navy faced a crisis of purpose after World War II. It had helped win the biggest conflict in history, but the Allied victory over the Axis powers was so sweeping that by 1954 the Navy had no viable rivals left to fight at sea. The Navy's longstanding strategic concept as the Nation's first line of defense no longer seemed compelling. In addition, the prospect of nuclear war had shaken strategic assumptions and was reshaping American foreign and defense policies. While no enemies could reach America's shores from the oceans, one adversary—the Soviet Union—could devastate the country from the skies with hydrogen bombs. The Navy's traditional "oceanic" orientation, which had justified powerful fleets, seemingly had little relevance for the application of American power against nuclear-armed land powers in Eurasia.

The Navy subsequently developed a "transoceanic" strategic concept, orienting the Service away from contesting the oceans and toward projecting power across them to distant land masses. In adapting its strategic concept to reflect changes in threats and national policy, the Navy ensured public confidence and support from Congress. The Navy's new strategic role endured through the Cold War, helping the United States maintain the forces that contained Soviet power and ensuring that America (with its allies) was so strong at sea that Moscow never seriously contemplated building fleets to rival ours.[2]

General Paul M. Nakasone, USA, is Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

When our nation asks, "What function does U.S. Cyber Command (USCYBERCOM) perform that obligates society to assume responsibility for its maintenance?" the command can reply that its strategic concept has evolved from a "response force" to a "persistence force." This persistence force will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace. Over time, a persistence force, operating at scale with U.S. and foreign partners, should raise the costs that our adversaries incur from hacking the United States. To protect our most critical public and private institutions from threats that continue to evolve in cyberspace, we cannot operate episodically.

While we cannot ignore vital cyber defense missions, we must take this fight to the enemy, just as we do in other aspects of conflict. A persistence force has a much higher chance of disrupting adversary plots and protecting Americans, compared with a force that is confined to sporadic reconnaissance. Persistence should not be mistaken for engagement for engagement's sake; instead, it is an approach that empowers U.S. cyber forces to achieve more decisive results in pursuit of objectives set by national leaders. This evolution aligns USCYBERCOM with changes in the strategic environment and in national policy as articulated in the 2017 National Security Strategy and 2018 National Defense Strategy.

Cyberspace and Great Power Competition

The growth of a global, interconnected cyberspace domain represents the biggest strategic development since 9/11. Activities and operations in, through, and from cyberspace now offer states the means to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition *without triggering armed conflict*. Our adversaries have learned this and are leveraging it against us.

When cyberspace went global in the 1990s, its fundamentals seemed to align comfortably with Western values. For this reason, its acceleration of social interaction, economic exchange, scientific progress, and military operations proved troubling to dictators who worried that their hold on power would be undermined by digital-age capabilities empowering civil society. The Arab Spring in 2011 heightened these fears. In response, increasingly cyber-capable governments escalated their operations against their own citizens and ours. They mounted global surveillance of opposing views and are stealing unprecedented quantities of intellectual property and personal data, disrupting democratic processes, holding critical infrastructure at risk, and eroding U.S. power. They employ technical activities that are individually inconsequential, yet cumulatively set the conditions for decisive advantage in conflict should it occur.

The return of great power competition prompted the authors of the new National Security Strategy to lament that while Americans "took [their] political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, [its] allies, and our partners." Growing political, economic, and military competitions around the world, according to the National Defense Strategy, are now the central challenge to U.S. security and prosperity. In these competitions, the locus of struggle for power has shifted toward cyberspace, and from open conflict to competitions below the level of armed attack.

Original Concept

USCYBERCOM began operations in 2010 when exploitation and disruption comprised the major cyber threats to Department of Defense (DOD) information networks and the Nation's critical infrastructure. Even though the United States had enjoyed general superiority in cyberspace since the creation of the domain, our competitors had developed and acquired effective, if often rudimentary, capabilities as well. The command's mission was to maintain U.S. superiority by checking the capability development of our competitors. USCYBERCOM initially focused on defending DOD networks and supporting geographic combatant commanders, particularly in Iraq and Afghanistan. USCYBERCOM was thus a *response* force—executing counterterrorism operations, planning to support conventional forces in crisis scenarios, and maintaining capacity to respond to an "attack of significant consequence" against our critical infrastructure.

In 2013, a year that marked a strategic inflection point and the obsolescence of that original strategic concept, surprisingly capable adversaries now operated continuously against critical infrastructure, government networks, defense industries, and academia—both in America and abroad. Cyber-enabled intellectual property theft had long been common, but now state-sponsored malicious activities began to impose significant costs on the Federal Government and private sector. The adversaries mounting these campaigns took care to operate in ways that would not trigger an armed U.S. response. Examples of their assaults included the Iranian denial-of-service attacks against the financial sector (2012–2013) and attack on the Sands Casino (2014), North Korea's attack on Sony Pictures Entertainment (2014), and China's disruption of GitHub (2015) and theft of security-related data from the Office of Personnel Management (2015). Russia raised cyberspace campaigns to a new level of boldness after 2015, launching a series of operations to interfere with the elections of the United States and its allies and sponsoring attacks on the Ukrainian power grid. These campaigns convinced even skeptics that cyberspace activities over time could cumulatively erode a country's sources of national power.

Today peer- and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns. Cyberspace provides our adversaries with new ways to mount continuous, nonviolent operations that produce cumulative, strategic impacts by eroding U.S. military, economic, and political power without reaching a threshold

that triggers an armed response. In other words, shifts in the global distribution of power can now occur without armed conflict. Hence the strategic concept of a response force—in effect, holding U.S. cyber forces in reserve for kinetic conflicts or responding after-the-fact to cyber attacks on America—resembles the Navy's pre-1945 strategic concept that Huntington critiqued. Worse still, it has had the effect of ceding the strategic initiative in cyberspace to adversaries willing to operate continuously against us. Continuous action in cyberspace for strategic effect has become the norm, and thus the command requires a new strategic concept.

A Cyber Persistence Force

We are learning how cyber capabilities can be employed to advance what the 2018 National Defense Strategy calls our "competition and wartime missions." Our adversaries are learning too, integrating and employing cyberspace capabilities in different ways consistent with their doctrine, strategy, organizational culture, and risk tolerance. History cautions that we should expect the use of new capabilities to evolve as they are introduced in conflicts. Tanks, for instance, developed from infantry support to deep penetration roles, while aircraft progressed from tactical reconnaissance to strategic bombing to unmanned intelligence, surveillance, and reconnaissance. With battlefield experience comes the evolution and maturation of operational concepts and strategic insights. Carl von Clausewitz noted that the "knowledge basic to the art of war is empirical," meaning theory must conform to experience.[3] USCYBERCOM has learned that successful engagement against adversaries in cyberspace requires that we continuously seek tactical, operational, and strategic initiative. Such persistence requires that we remain ahead of them both in knowledge and in action. It also demands that we leverage our strengths across intelligence and operations to achieve this end.

In March 2018, USCYBERCOM's command vision document, *Achieve and Maintain Cyberspace Superiority*, updated the command's strategic concept to align with changes in national strategy and in the cyberspace competition.[4] The document acknowledges that the locus of struggle in the revived great-power competition has shifted toward cyberspace and that decisive action can occur below the level of armed attack. Its strategic concept is "cyber persistence" rather than "cyber response," empowering USCYBERCOM to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way.

USCYBERCOM's strategic thinking is evolving along with our forces and capabilities. We are accelerating change in the following ways:

- We are shifting our strategic perspective away from viewing war and territorial aggression as the only perils for our national sources of power. A byproduct of successfully deterring conventional and nuclear war is that adversaries now shape America's policy choices through cyberspace operations calibrated to avoid provoking armed responses. Because our adversaries still feel able to operate against the United States and its interests through cyberspace, and because historically there has been little cost imposed for doing so, USCYBERCOM must operate below traditional use-of-force thresholds while also preparing to be a lethal force in conflict.
- We are building relationships with U.S. institutions that are likely to be targets of foreign hacking campaigns—particularly in the Nation's critical infrastructure—before crises develop, replacing transactional relationships with continuous operational collaboration among other departments, agencies, and the private sector. These relationships are crucial to thwarting attackers before they strike and to increasing resilience after a successful breach. Ideally, these partnerships will allow our persistence force to address patterns of malicious cyber behavior before they become attacks.
- We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace. Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks. To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment.
- We have shifted away from the earlier emphasis on holding targets "at risk" for operations at a time and place of our choosing. We will operate continuously to present our decisionmakers with up-to-date options. Cyberspace targets themselves typically amount to computer and data "states," which change constantly in the normal functioning of digital information systems. Successful operations require capabilities and tactics that can rapidly shift from unsuccessful approaches in order to exploit new vulnerabilities and opportunities.
- Finally, we are ensuring our capabilities, operational tempo, decisionmaking processes, and authorities enable continuous, persistent operations. Adversaries and competitors have responded to our restrained and episodic engagement with cyber aggression that has eroded U.S. military, economic, and diplomatic advantages. Strategic effects in cyberspace come from the use—not the mere possession—of cyber capabilities to gain the initiative over those who mean us harm.

Airmen gather around computer at first U.S. Air Forces in Europe cyber-only exercise Tacet Venari at Warrior Preparation Center on Einsiedlerhof Air Station, Germany, May 10, 2018 (U.S. Air Force/Blake Browning)

The Value of the Cyber Force

Senior political and military leaders recognize that our military must be able to compete below the level of armed conflict, and this idea is clearly stated in the National Security Strategy: "Our task is to ensure that American military superiority endures, and in combination with other elements of national power, is ready to protect Americans against sophisticated challenges to national security."[5] Nowhere is this requirement greater than in cyberspace, where peer competitors operate continuously against us in search of strategic advantage. To meet this intent, USCYBERCOM will:

- Operate forward and at scale where our adversaries are. This is the primary mission of cyber forces, which gives rise to U.S. Cyber Command's concept of defend forward. Its purpose is to limit the terrain over which the enemy can gain influence or control. We cannot afford to let adversaries breach our networks, systems, and data (intellectual property and personally identifiable information). If we are only defending in "blue space," we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.
- Assure the joint force can conduct operations securely and reliably. USCYBERCOM defends the DOD Information Network (DODIN), which is the command, control, communications, and data hub for the joint force. It facilitates nearly every phase of operations for the U.S. military. By defending the DODIN, USCYBERCOM has indirectly but strongly supported virtually every U.S. military operation launched since 2010. DOD relies on an increasingly secure and resilient information network to meet its full range of warfighting and enabling functions *because of past and ongoing USCYBERCOM operations.*

Enabling Capabilities for a Persistence Force

We are at a transformational moment for U.S. strategy and operations in cyberspace. Cyberspace represents a new strategic environment through which relative power can be challenged without resorting to armed conflict. Senior political and military leaders recognize that the initial approach that DOD took toward cyberspace aggression—focusing on resiliency and response actions—in effect committed the fundamental flaw in military operations of holding one's forces in reserve past the point of decision.

Fire controlman assigned to C4 cyber and intelligence department aboard USS *America* inspects surface-to-air intercept missile 162D on ship's missile deck, Pacific Ocean, August 31, 2017 (U.S. Navy/Alexander A. Ventura II)

Huntington identifies two other important factors that determine the success of a strategic concept: the resources, both human and material, required to implement it, and the organizational structure, which groups the resources allocated by society in a manner that implements the strategic concept. USCYBERCOM is maturing as a combatant command with the teams, infrastructure, tools, accesses, and authorities ready to execute missions. The command is also transitioning from force generation to a sustained readiness approach for persistent engagement with cyber adversaries and increased lethality in war. We continue to evolve the organization based on operational experience, task organizing, and employing small elements of teams in ways never anticipated when we stood them up.

One last factor that is crucial to success of a military element's strategic concept, which Huntington implied in his 1954 essay, is the ability of the commanders and the force itself to instill a sense of confidence among civilian leaders and the larger public that the element has devised an appropriate and viable strategic concept and has the skills to execute it on behalf of the Nation. The actions that follow from the strategic concept of persistent engagement should, over time, allow USCYBERCOM to install that sense of confidence. **JFQ**

Notes

[1] Samuel P. Huntington, "National Policy and the Transoceanic Navy," U.S. Naval Institute *Proceedings* 80, no. 5 (May 1954).

[2] The Soviets had built a powerful navy by the 1980s, but they used it to control their local seas and protect their strategic missile submarines—not to contest control of the Atlantic or Pacific.

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 170.

[4] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018).

[5] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 3.